

Appl. No. 09/745,488

Amdt. Dated: May 21, 2004

Reply to Office Action of: 11/23/2003

### Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

#### Listing of claims:

1. (currently amended) A method of establishing a common shared key between a pair of correspondents, said method comprising the steps of exchanging a pair of messages between the correspondents with one message from each of the correspondents, each of the messages having a portion signed by a sender and including the identity of the intended recipient and including identification information in said messages said sender and intended recipient thereby information being identifiable to one or other of said correspondents to thereby establish said common key between intended parties.
2. (currently amended) A method as defined in claim 1, including the steps of providing in said signed portion identities of the sender and the receiver including a flow number in a message to be signed.
3. (original) A method as defined in claim 1, said step of exchanging messages being based on a STS-MAC Protocol.
4. (original) A method as defined in claim 3, including the step of transmitting the sender's certificate in a first flow to thereby minimize an on-line UKS attack against a recipient.
5. (original) A method as defined in claim 1, including the step of providing the identities of the correspondents in a key derivation function rather than a signed message.
6. (original) A method as defined in claim 1, said exchange of messages being based on an STS-ENC Protocol.
7. (original) A method as defined in claim 1, said exchange of messages being based on an STS-MAC Protocol.

020488-319434

McCarthy Tétrault LLP TDO-RED #8232044 p. 1